明　細　書

コンテンツ配信システム

技術分野

本発明は、コンテンツを配信する技術に関し、特に、コンテンツの配信を許可する端末を判断する技術に関する。

背景技術

近年、家庭内の端末をネットワークで接続し、接続された端末間でコンテンツの共有を図る家庭内ネットワークが実現されつつある。

家庭内ネットワークの実現形態の一つとして、家庭内にルータを１台設け、そのルータ下にＤＶＤレコーダやビデオなどの各端末と、コンテンツを蓄積するコンテンツサーバとを接続する形態が考えられる。ルータは、家庭内において唯一家庭外のネットワークに接続されており、コンテンツサーバは、ルータを介して家庭外のネットワークからコンテンツを取得し、取得したコンテンツを蓄積する。各端末は、コンテンツサーバへコンテンツを要求し、コンテンツサーバは、端末からの要求に応じて、コンテンツを配信する。

しかしながら、著作権保護の観点より、コンテンツを無制限に配信することは認められない。従って、家庭内の端末のみに利用が許可されたコンテンツは、家庭外の端末に配信されないよう制限されなければならない。

そこで、特許文献１には、送信装置と受信装置とが同一のサブネットアドレスを有する場合に、認証及び鍵交換を実行してコンテンツを送受信する技術が開示されている。

上記の技術により、同一のサブネットアドレスを有する端末間でのみ、コンテンツを送受信することが可能であるが、同一のサブネットアドレスを有する端末間であっても、通信途中で第三者にコンテンツを盗まれる危険度が高い状況などでは、コンテンツの送受信を抑制したいという要望がある。

【特許文献１】特開２００１－２８５２８４号公報

発明の開示

そこで、本発明は、上記の要望に鑑みなされたものであって、通信途中で第三者にコンテンツを盗まれる危険度が高い状況では、コンテンツの送受信を抑制するコンテンツ配信システムを提供することを目的とする。

上記目的を達成するために本発明は、本発明は、通信装置であって、前記通信装置と他の通信装置とのデータ通信における隔たりの量を示す通信距離を取得し、取得した前記通信距離が、所定値以下であるか否か判定し、前記判定の結果が肯定的である場合に、前記他の通信装置との間でコンテンツの送信又は受信を行うことを特徴とする。

この構成によると、他の通信装置とのデータ通信における隔たりの量と、前記所定値とに応じてコンテンツを送受信したり、コンテンツの送受信を抑制したりできる。

ここで、前記通信装置は、前記コンテンツの送信又は受信に先立ち、前記他の通信装置とデータの通信を行い、前記他の通信装置から送信されたデータを当該通信装置が受信するまでの間に、前記データが経由した中継機器の数を示す前記通信距離を取得するように構成してもよい。

この構成によると、他の通信装置とのデータ通信においてデータが経由した中継機器の数と、前記所定値とに応じてコンテンツを送受信したり、コンテンツの送受信を抑制したりできる。

ここで、前記通信装置は、前記他の通信装置から送信されたデータを当該通信装置が受信するまでの間に、前記データが経由した中継機器の数として、前記データが経由したルータの数を示す前記通信距離を取得するように構成してもよい。

この構成によると、他の通信装置とのデータ通信においてデータが経由した値ルータの数と、前記所定値とに応じてコンテンツを送受信したり、コンテンツの送受信を抑制したりできる。

ここで、前記通信装置は、ルータを一つ経由する毎に１ずつ値が減少する性質を有するＴＴＬ（Time To Live）を含むパケットの形式で、前記データの通信を行い、受信するパケットに含まれる前記ＴＴＬを用いて、前記データが経由したルータの数を示す前記通信距離を取得するように構成してもよい。

この構成によると、データが経由したルータの数を取得する取得方法として、ＩＰパケットのＴＴＬフィールドに設定されるＴＴＬを用いることで、既存の通信プロトコルを用いて本発明を実施することができる。

ここで、前記通信装置は、更に、前記他の通信装置と鍵情報を共有するように構成してもよいし、また、前記通信装置は、更に、前記他の通信装置と共有した前記鍵情報を用いて、前記コンテンツの暗号化処理及び暗号化された前記コンテンツの復号処理を行い、前記他の通信装置との間で、暗号化された前記コンテンツの送信又は受信を行うように構成してもよい。

この構成によると、他の通信端末との間で鍵共有処理を行い、当該通信端末と他の通信端末との間で、共有した鍵情報を用いてセキュアにコンテンツを送受信することができる。

ここで、前記通信装置は、前記他の通信装置から、当該他の通信装置が接続されている第１のルータを一意に識別する第１識別情報を含む前記パケットを受信し、更に、当該通信装置が接続されている第２のルータを一意に識別する第２識別情報を取得し、前記第１識別情報と前記第２識別情報とが一致するか否か判断し、前記判断の結果が否定的である場合に前記コンテンツの送受信を抑制するように構成してもよい。

この構成によると、接続されている中継機器の識別情報を取得して判断することにより、確かに同一の中継機器に接続された通信装置間でコンテンツを送受信することができ、外部にコンテンツが流出するのを抑制することができる。

ここで、前記通信装置が送受信する各パケットは、当該通信装置が接続されているネットワークの最大伝送量（Maximum Transmission Unit）に等しいデータサイズであり、且つ、分割して送受信することが禁止されているように構成してもよい。

この構成によると、前記他の通信装置が、ＩＰパケットの外側に新しいＩＰヘッダを付加して実際に指定された数のＴＴＬと異なるＴＴＬを設定して送信しようとする場合に、既にパケットがＭＴＵに等しいサイズであるため、新たなＩＰヘッダを付加するとパケットを分割送信しなくてはならない。しかしながら、この構成により、パケットの分割送信は禁止されているため、結局不正なパケットは当該通信

装置に届かない。

ここで、前記通信装置は、前記他の通信装置から、送信時に所定ＴＴＬが設定されて送信されたパケットを受信し、受信した前記パケットからＴＴＬを読み、読み出したＴＴＬと前記所定ＴＴＬとの差分である前記通信距離を取得するように構成してもよい。

この構成によると、予め、他の通信装置に所定ＴＴＬを通知しておくことで、受信したパケットに含まれるＴＴＬを読み出すことで、容易にデータが経由したルータの数を取得することができる。

ここで、前記通信装置は、前記他の通信装置から、送信時に前記所定ＴＴＬとして「１」が設定されて送信された前記パケットを受信するように構成してもよい。

この構成によると、他の通信装置から、ＴＴＬが「１」に設定されたパケットが送信されるため、当該通信装置が、パケットを受信した場合、前記パケットは、他のネットワークのルータを経由せずに他の通信装置から当該通信装置へ送信されたことが分かる。即ち、当該通信装置と前記他の通信端末とが同一のルータ下に接続されていることが分かる。

ここで、前記通信装置は、一部又は全部が暗号化されたパケットを送信又は受信し、受信したパケットを復号して各処理を行い、又は、送信されるパケットを暗号化して出力するように構成してもよい。

この構成によると、判定に用いるデータであるパケットの一部又は全部が暗号化されているため、前記データをセキュアに送受信することができる。

図面の簡単な説明

図１は、コンテンツ配信システム１の構成を示す図である。

図２は、コンテンツサーバ２０の構成を機能的に示す機能ブロック図である。

図３は、端末３０の構成を機能的に示す機能ブロック図である。

図４（ａ）は、コンテンツサーバ検索パケット３０１のデータ構造を示す図である。

（ｂ）は、確認パケット３０２のデータ構造を示す図である。

（ｃ）は、鍵共有要求パケット３０３のデータ構造を示す図である。

図５は、コンテンツ配信システム１の動作を示すフローチャートである。

図６は、コンテンツ配信システム１におけるＡＤ判定処理の動作を示すフローチャートであり、図７に続く。

図７は、コンテンツ配信システム１におけるＡＤ判定処理の動作を示すフローチャートであり、図６から続く。

図８は、コンテンツ配信システム１における鍵共有処理の動作を示すフローチャートである。

図９（ａ）は、コンテンツ配信システム１におけるコンテンツ送信処理の動作を示すフローチャートである。

（ｂ）は、コンテンツ配信システム１におけるコンテンツ受信処理の動作を示すフローチャートである。

図１０は、コンテンツ配信システム１ａの構成を示す図である。

図１１は、端末３０ｂの構成を機能的に示す機能ブロック図である。

図１２は、ＴＴＬ検索パケット３０４のデータ構造を示す図である。

図１３は、コンテンツ配信システム１ａの動作を示すフローチャートである。

図１４は、コンテンツ配信システム１ａにおけるＴＴＬ検索処理の動作を示すフローチャートである。

図１５は、コンテンツ配信システム１ａにおけるＡＤ判定処理の動作を示すフローチャートであり、図１６に続く。

図１６は、コンテンツ配信システム１ａにおけるＡＤ判定処理の動作を示すフローチャートであり、図１５から続く。

図１７は、コンテンツ配信システム１ｂの構成を示す図である。

図１８は、コンテンツサーバ２０ｂの構成を機能的に示す機能ブロック図である。

図１９は、端末３０ｃの構成を機能的に示す機能ブロック図である。

図２０（ａ）は、公開鍵パケット３０５のデータ構造を示す図である。

（ｂ）は、公開鍵パケット３０６のデータ構造を示す図である。

図２１は、コンテンツ配信システム１ｂの全体の動作を示すフローチャートである。

図２２は、コンテンツ配信システム１ｂにおける鍵共有処理の動作を示すフロー

チャートである。

図２３は、コンテンツ配信システム２の構成を示す図である。

図２４は、コンテンツサーバ２０ａの構成を機能的に示す機能ブロック図である。

図２５は、グループテーブル３５０のデータ構造を示す図である。

図２６（ａ）は、コンテンツ配信システム２の動作を示すフローチャートである。

（ｂ）は、コンテンツ配信システム２におけるコンテンツ要求処理の動作を示すフローチャートである。

発明を実施するための最良の形態

以下、本発明の実施の形態について詳細に説明する。

≪第１の実施の形態≫

本発明に係る第１の実施の形態として、コンテンツ配信システム１について図面を参照して説明する。コンテンツ配信システム１は、コンテンツの利用が許可された範囲において、機器間でコンテンツを送受信するシステムである。以下では、コンテンツの利用が許可された範囲を「ＡＤ（Authorized Domain）」と呼称する。また、以下では、特にＡＤとして、家庭内ネットワークに接続された家庭内の機器を想定している。

＜構成＞

図１は、コンテンツ配信システム１の構成を示す図である。同図に示す様に、コンテンツ配信システム１は、ルータ１０、ルータ１１、ルータ１２、コンテンツサーバ２０、端末３０、端末４０及び端末５０から構成される。

インターネット６０に接続されたルータ１０には、ルータ１１及びルータ１２が接続されている。ルータ１１は、ＡＤ内に存在する中継機器であり、ルータ１２はＡＤ外に存在する中継機器である。ルータ１１には、コンテンツサーバ２０と端末３０とが接続されており、ルータ１２には、端末４０と端末５０とが接続されている。

なお、コンテンツ配信システム１において、ＡＤ内の各端末は、一つのルータ下に接続されているものとする。また、コンテンツ配信システム１において、各機器は通信プロトコルとしてＩＰｖ４を使用して通信を行うものとする。

１．コンテンツサーバ２０の構成

コンテンツサーバ２０は、他の機器からの要求を受け、前記機器がＡＤ内の機器であるか、又は、ＡＤ外の機器であるか判断する。判断の結果、前記機器がＡＤ内の機器である場合に、コンテンツサーバ２０は、前記機器と鍵共有処理を行い、共有した鍵を用いて暗号化したコンテンツを前記機器へ送信する。

なお、以下では、ＡＤ内の機器であると判断された端末を、「グループ内端末」又は「グループメンバ」と呼称することがある。

図２は、コンテンツサーバ２０の構成を機能的に示した機能ブロック図である。同図に示す様に、コンテンツサーバ２０は、通信部１０１、暗号処理部１０２、機器ＩＤ管理部１０３、中継機器固有情報取得部１０４、最大伝送量探査部１０５、ＡＤ判定部１０６、確認情報生成部１０７、共有鍵生成部１０８及びコンテンツ格納部１０９から構成される。

コンテンツサーバ２０は、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、ハードディスクユニット、ネットワーク接続ユニット、ディスプレィユニット、リモートコントローラなどから構成されるコンピュータシステムであって、ここでは、ＨＤＤレコーダを想定している。

前記ＲＡＭ又は前記ハードディスクユニットにはコンピュータプログラムが記憶されており、前記マイクロプロセッサが、前記コンピュータプログラムに従い動作することにより、コンテンツサーバ２０は、各種の機能を達成する。

（１）通信部１０１

通信部１０１は、ルータ１１を介してＩＰパケットを送受信することにより他の機器と通信を行う通信インターフェースである。

通信部１０１は、暗号処理部１０２によりＩＰペイロードが暗号化された送信用パケットを順次受け取り、受け取った送信用パケットをルータ１１へ送出する。送信用パケットの一例は、図４（ｂ）に示した確認パケット３０２である。また、通信部１０１は、暗号処理部１０２により暗号化された送信情報を受け取り、受け取った送信情報を分割して送信用パケットを生成し、生成した送信用パケットを順次ルータ１１へ送出する。送信情報の具体例は、暗号化コンテンツ、コンテンツサーバ２０の公開鍵等である。なお、通信部１０１は、送信情報を分割して送信用パケ

ットを生成する際、パケットサイズが、ＭＴＵ（Maximum Transmission Unit；伝送路の最大転送サイズ）に等しくなるようパディング処理を行う。ここで、ＭＴＵは、最大伝送量探査部１０５から受け取る情報である。

また、通信部１０１は、ルータ１１から暗号化されたＩＰペイロードを含む受信用パケットを受信し、受信した受信用パケットを順次暗号処理部１０２に出力する。受信用パケットの具体例は、図４（ａ）に示したコンテンツサーバ検索パケット３０１、同図（ｃ）に示した鍵共有要求パケット３０３などである。また、通信部１０１は、ルータ１１から暗号化されたＩＰペイロードを含む受信用パケットを受信して蓄積し、受信情報を生成する。通信部１０１は、生成した受信情報を暗号処理部１０２へ出力する。受信情報の具体例は、端末の公開鍵等である。

なお、コンテンツサーバ検索パケット３０１、確認パケット３０２及び鍵共有要求パケット３０３の具体的なデータ構造等については後述する。

（２）暗号処理部１０２

暗号処理部１０２は、確認情報生成部１０７から、順次確認パケットを受け取り、受け取った確認パケットのＩＰペイロードを暗号化した後、通信部１０１へ出力する。暗号処理部１０２は、共有鍵生成部１０８からコンテンツサーバ２０の公開鍵を受け取り、受け取った公開鍵を暗号化した後、通信部１０１へ出力する。

また、暗号処理部１０２は、通信部１０１からコンテンツサーバ検索パケットを順次受け取り、受け取ったコンテンツサーバ検索パケットのＩＰペイロードを復号したのち、ＡＤ判定部１０６へ出力する。暗号処理部１０２は、通信部１０１から鍵共有要求パケットを順次受け取り、受け取った鍵共有要求パケットのＩＰペイロードを復号してＡＤ判定部１０６へ出力する。

このとき暗号処理部１０２が行う暗号化及び復号処理のアルゴリズムの一例は、秘密鍵暗号方式ＡＥＳ（Advanced Encryption Standard）であり、ここで用いる鍵情報は、予め、通信を行う機器との間で共有しているものとする。また、鍵情報は耐タンパ性領域に格納されているものとする。なお、ＡＥＳについては、ＦＩＰＳ（Federal Information Processing Standard）－１９７で定義されているため説明を省略する。

更に、暗号処理部１０２は、コンテンツ格納部１０９からコンテンツを受け取り、

共有鍵生成部１０８に格納されている共有鍵を読み出す。暗号処理部１０２は、読み出した共有鍵を用いてコンテンツを暗号化し、暗号化コンテンツを生成する。暗号処理部１０２は、生成した暗号化コンテンツを通信部１０１へ出力する。このとき暗号処理部１０２が行う暗号化処理のアルゴリズムの一例は、ＡＥＳである。

（３）機器ＩＤ管理部１０３

機器ＩＤ管理部１０３は、コンテンツサーバ２０を一意に識別するために用いられる機器ＩＤ「ＩＤ＿Ａ」を格納している。「ＩＤ＿Ｂ」は、具体的には、コンテンツサーバ２０に固有の８バイトデータである。

（４）中継機器固有情報取得部１０４

中継機器固有情報取得部１０４は、コンテンツサーバ２０が接続されているルータのＭＡＣアドレスを取得して、内部の記憶領域に格納する。なお、中継機器固有情報取得部１０４は、コンテンツサーバ２０が初めてルータに接続されたとき、上記の処理を行うように構成してもよいし、また、定期的にコンテンツサーバ２０が接続されているルータのＭＡＣアドレスを取得し、記憶領域に格納されているＭＡＣアドレスに上書きするように構成してもよい。

なお、ＭＡＣアドレスの取得方法の一例は、ＡＲＰ（Address Resolution Protocol）である。ＡＲＰについては、ＲＦＣ（Request For Comment）８２５で説明されているため、説明を省略する。

（５）最大伝送量探査部１０５

最大伝送量探査部１０５は、コンテンツサーバ２０が接続されているネットワークの最大伝送量を取得して、取得した最大伝送量を内部の記憶領域に格納する。なお、最大伝送量探査部１０５は、コンテンツサーバ２０が初めてネットワークに接続されたとき１回のみ上記処理を行うように構成してもよいし、定期的にコンテンツサーバ２０が接続されているネットワークの最大伝送量を取得し、記憶領域に格納されている最大伝送量に上書きするように構成してもよい。

なお、最大伝送量の取得方法としては、ＲＦＣ１１９１で説明されている経路ＭＴＵ探索の方法を用いる。

（６）ＡＤ判定部１０６

ＡＤ判定部１０６は、他の機器からコンテンツの要求を受けて、当該他の機器が

ＡＤ内の機器であるか否かを判定する。

ＡＤ判定部１０６は、コンテンツサーバ２０が初めてネットワークに接続されたときインターネット６０を介して、発行機関からＣＲＬ(Certification Revocation List）を受信し、記憶する。ＣＲＬは、秘密鍵が暴露された機器など、無効化された機器の機器ＩＤが登録されているリストである。ＡＤ判定部１０６は、インターネット６０を介して、発行機関から常に最新のＣＲＬを受信し、それまで記憶していたＣＲＬに上書きする。

ＡＤ判定部１０６は、暗号処理部１０２から、コンテンツサーバ検索パケットを受け取ったとき、及び、鍵共有要求パケットを受け取ったとき、以下の（判断１）から（判断３）までの処理を行う。

（判断１）ＡＤ判定部１０６は、コンテンツサーバ検索パケット及び鍵共有要求パケットから機器ＩＤを読み出し、読み出した機器ＩＤが、内部に記憶しているＣＲＬに記載されておらず、送信元端末が無効化されていないか否か判断する。

（判断２）次に、ＡＤ判定部１０６は、コンテンツサーバ検索パケット及び鍵共有要求パケットからＴＴＬを読み出し、読み出したＴＴＬが「１」であるか否か判断する。

（判断３）次に、ＡＤ判定部１０６は、コンテンツサーバ検索パケット及び鍵共有要求パケットから中継機器固有情報を読み出す。また、ＡＤ判定部１０６は、中継機器固有情報取得部１０４が記憶している中継機器固有情報を読み出す。ＡＤ判定部１０６は、読み出した２個の中継機器固有情報が同一であるか否か判断する。

コンテンツサーバ検索情報に対する上記１、２、及び３の判断において、全てが肯定的である場合に、ＡＤ判定部１０６は、当該コンテンツサーバ検索パケットを送信した端末へ送信する確認パケットを生成する指示を、確認情報生成部１０７へ出力する。

鍵共有要求パケットに対する上記１、２及び３の判断において、全てが肯定的である場合に、ＡＤ判定部１０６は、当該鍵共有要求パケットを送信した端末との間で共有鍵を生成する指示を、共有鍵生成部１０８へ出力する。

ここで、「ＴＴＬ（Time To Live）」は、ネットワーク上に送出されたパケットが、ルータの設定ミスなどによりループになってしまった場合に、パケットがネ

ットワーク上に生存し続けることを防ぐため、パケットの生存可能時間を表すものである。具体的には、ホップカウントをもってＴＴＬとする。端末は、パケット送信時に、所定のＴＴＬをＩＰヘッダのＴＴＬフィールドに設定する。設定されたＴＴＬは、パケットがルータを通過して次の中継機器であるルータに送出される毎に１ずつデクリメントされる。ＴＴＬが０になるとパケットはルータによって破棄され、それ以上転送されない。

（７）確認情報生成部１０７

確認情報生成部１０７は、ＡＤ判定部１０６からの指示を受けて、以下に示す様に確認パケットを生成する。確認パケットは、ＩＰヘッダとＩＰペイロードとから構成される。以下では、図４（ｂ）に示した確認パケット３０２を例に説明する。

ＩＰヘッダは、ＤＦ（Don' t Fragment）ビット、ＴＴＬ、及び宛先アドレスを含む。ＤＦビットは、「有効」又は「無効」の何れかに設定される。「有効」はフラグメントが禁止されていることを示し、「無効」はフラグメントが許可されていることを示す。フラグメントとは、パケットを分割して送信する機能である。図４（ｂ）に示す様に、確認情報生成部１０７は、ＤＦビットを「有効」に設定し、フラグメントを禁止することで、所謂「カプセル化」を抑止する。確認情報生成部１０７は、ＴＴＬを「１」に設定し、確認パケット３０２が、ルータ１１を越えて他のネットワークへ送出されることを抑止する。確認情報生成部１０７は、コンテンツサーバ検索パケットを送信した送信元端末のＩＰアドレスを、宛先アドレスとする。送信元端末のＩＰアドレスは、送信元端末の機器ＩＤと対応付けて、予め確認情報生成部１０７が記憶していてもよいし、送信元端末から送信されるパケットに含まれており、確認情報生成部１０７がパケットからＩＰアドレスを抽出するように構成されてもよい。

ＩＰペイロードは、パケット種別、コンテンツサーバドレス、中継機器固有情報及びパディングデータを含む。確認情報生成部１０７は、当該パケットが確認パケットであることを示す為に、パケット種別として「確認」を書き込む。確認情報生成部１０７は、コンテンツサーバドレスとして、自身のＩＰアドレスを書き込む。確認情報生成部１０７は、中継機器固有情報取得部１０４からルータのＭＡＣアドレスを読み出し、読み出したＭＡＣアドレスを、中継機器固有情報として書き込む。

確認情報生成部１０７は、確認パケット３０２のデータサイズがＭＴＵに等しくなるよう、パディングデータを書き込む。ここでは、例としてパディングデータは「０」である。

確認情報生成部１０７は、上記の様に生成した確認パケット３０２を、順次暗号処理部１０２へ出力する。

（８）共有鍵生成部１０８

共有鍵生成部１０８は、予め、外部の管理センタから楕円曲線Ｅ：ｙ＝ｘ^{3}＋ａｘ＋ｂと元Ｇとが与えられているものとする。

共有鍵生成部１０８は、ＡＤ判定部１０６から、鍵共有要求パケットを送信した端末との間で共有鍵を生成する指示を受け取ると、以下に示す様にして、共有鍵生成処理を行う。

共有鍵生成部１０８は、秘密鍵ｘＡを設定して次式により公開鍵ＹＡを算出する。

ＹＡ＝ｘＡ＊Ｇ

共有鍵生成部１０８は、算出した公開鍵ＹＡを、送信元端末へ送信すると共に、送信元端末から、送信元端末の公開鍵ＹＢを受信する。

共有鍵生成部１０８は、受信した送信元端末の公開鍵ＹＢと自身の秘密鍵とから、ｘＡ＊ＹＢを算出することにより共有鍵を生成し、生成した共有を内部に記憶する。

共有鍵生成部１０８は、共有鍵を生成して記憶すると、コンテンツ格納部１０９に対して、コンテンツを読み出す指示を出力する。

（９）コンテンツ格納部１０９

コンテンツ格納部１０９は、具体的にはハードディスクドライブユニットであって、内部にコンテンツを格納している。共有鍵生成部１０８からの指示を受けて、読み出したコンテンツを暗号処理部１０２へ出力する。

２．端末３０の構成

端末３０は、ルータ１１に接続されたＡＤ内の機器であり、ルータ１１を介してコンテンツサーバ２０との間で鍵共有処理を行い、共有鍵を用いてコンテンツの送受信を行う。

図３は、端末３０の構成を機能的に示す機能ブロック図である。同図に示す様に、端末３０は、通信部２０１、暗号処理部２０２、機器ＩＤ管理部２０３、中継機器

固有情報取得部２０４、最大伝送量探査部２０５、コンテンツサーバ検索情報生成部２０６、鍵共有要求情報生成部２０７、共有鍵生成部２０８及び記憶部２０９から構成され

端末３０は、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、ハードディスクユニット、ネットワーク接続ユニット、ディスプレィユニット、リモートコントローラなどから構成され、より具体的には、端末３０は、ネットワークに接続可能なＡＶ機器や家電製品などである。前記ＲＡＭ又は前記ハードディスクユニットにはコンピュータプログラムが記憶されており、前記マイクロプロセッサが、前記コンピュータプログラムに従い動作することにより、端末３０は、各種の機能を達成する。

（１）通信部２０１

通信部２０１は、ルータ１１を介してＩＰパケットを送受信することにより他の機器と通信を行う通信インターフェースである。

通信部２０１は、暗号処理部２０２によりＩＰペイロードが暗号化された送信用パケットを順次受け取り、受け取った送信用パケットをルータ１１へ送出する。送信用パケットの具体例は、図４（ａ）に示したコンテンツサーバ検索パケット３０１、同図（ｃ）に示した鍵共有要求パケット３０３等である。また、通信部２０１は、暗号処理部２０２により暗号化された送信情報を受け取り、受け取った送信情報を分割して送信用パケットを生成し、生成した送信用パケットを順次ルータ１１へ送出する。送信情報の具体例は、端末３０の公開鍵等である。なお、通信部２０１は、送信情報を分割して送信用パケットを生成する際、パケットサイズが、ＭＴＵに等しくなるようパディング処理を行う。ここで、ＭＴＵは、最大伝送量探査部２０５から受け取る情報である。

また、通信部２０１は、ルータ１１から暗号化されたＩＰペイロードを含む受信用パケットを受信し、受信した受信用パケットを順次暗号処理部２０２に出力する。受信用パケットの具体例は、図４（ｂ）に示した確認パケット３０２などである。また、通信部２０１は、ルータ１１から暗号化されたＩＰペイロードを含む受信用パケットを受信して蓄積し、受信情報を生成する。通信部２０１は、生成した受信情報を暗号処理部２０２へ出力する。受信情報の具体例は、暗号化コンテンツなど

である。

（２）暗号処理部２０２

暗号処理部２０２は、コンテンツサーバ２０の暗号処理部１０２と同様の構成及び機能を有する。

暗号処理部２０２は、コンテンツサーバ検索情報生成部２０６から、順次コンテンツサーバ検索パケットを受け取り、受け取ったコンテンツサーバ検索パケットのＩＰペイロードを暗号化した後、通信部２０１へ出力する。同様に、暗号処理部２０２は、鍵共有要求情報生成部２０７から鍵共有要求パケットを受け取り、受け取った鍵共有要求パケットのＩＰペイロードを暗号化した後、通信部２０１へ出力する。また、暗号処理部２０２は、共有鍵生成部２０８から端末３０の公開鍵を受け取り、受け取った公開鍵を暗号化した後、通信部２０１へ出力する。

また、暗号処理部２０２は、通信部２０１から確認パケットを順次受け取り、受け取った確認パケットのＩＰペイロードを復号したのち、鍵共有要求情報生成部２０７へ出力する。

このとき暗号処理部２０２が行う暗号化及び復号処理のアルゴリズムの一例は、秘密鍵暗号方式ＡＥＳであり、ここで用いる鍵情報は、予め、コンテンツサーバ２０との間で共有しているものとする。また、鍵情報は耐タンパ性領域に格納されているものとする。

更に、暗号処理部２０２は、通信部２０１から暗号化コンテンツを受け取り、共有鍵生成部２０８に格納されている共有鍵を読み出す。暗号処理部２０２は、読み出した共有鍵を用いて暗号化コンテンツを復号し、コンテンツを生成する。暗号処理部２０２は、生成したコンテンツを記憶部２０９に格納する。

（３）機器ＩＤ管理部２０３

機器ＩＤ管理部２０３は、端末３０を一意に識別するために用いられる機器ＩＤ「ＩＤ＿Ｂ」を格納している。「ＩＤ＿Ｂ」は、具体的に、端末３０に固有の８バイトデータである。

（４）中継機器固有情報取得部２０４

中継機器固有情報取得部２０４は、端末３０が接続されているルータのＭＡＣアドレスを取得して、内部の記憶領域に格納する。なお、中継機器固有情報取得部２

０４は、端末３０が初めてルータに接続されたとき、上記の処理を行うように構成してもよいし、また、定期的に端末３０が接続されているルータのＭＡＣアドレスを取得し、記憶領域に格納されているＭＡＣアドレスに上書きするように構成してもよい。なお、ＭＡＣアドレスの取得方法の一例は、ＡＲＰである。

（５）最大伝送量探査部２０５

最大伝送量探査部２０５は、端末３０が接続されているネットワークの最大伝送量を取得して、取得した最大伝送量を内部の記憶領域に格納する。なお、最大伝送量探査部２０５は、端末３０が初めてネットワークに接続されたとき１回のみ上記の処理を行うように構成してもよいし、定期的に端末３０が接続されているネットワークの最大伝送量を取得し、記憶領域に格納されている最大伝送量に上書きするように構成してもよい。

なお、最大伝送量の取得方法としては、ＲＦＣ１１９１で説明されている経路ＭＴＵ探索の方法を用いる。

（６）コンテンツサーバ検索情報生成部２０６

コンテンツサーバ検索情報生成部２０６は、要求が発生すると、以下に示す様にコンテンツサーバ検索パケットを生成する。コンテンツサーバ検索パケットは、ＩＰヘッダとＩＰペイロードとから構成される。以下では、図４（ａ）に示したコンテンツサーバ検索パケット３０１を例に説明する。

ＩＰヘッダは、ＤＦビット、ＴＴＬ、及び宛先アドレスを含み、コンテンツサーバ検索情報生成部２０６は、ＤＦビットを「有効」に設定し、フラグメントを禁止する。コンテンツサーバ検索情報生成部２０６は、ＴＴＬを「１」に設定する。また、コンテンツサーバ検索情報生成部２０６は、マルチキャストアドレスを宛先アドレスとする。なお、コンテンツサーバ検索情報生成部２０６が設定するＴＴＬは、予めコンテンツサーバ２０から通知されているものとする。

ＩＰペイロードは、パケット種別、機器ＩＤ、中継機器固有情報及びパディングデータを含む。コンテンツサーバ検索情報生成部２０６は、当該パケットがコンテンツサーバ検索パケットであることを示す為に、パケット種別として「コンテンツサーバ検索」を書き込む。コンテンツサーバ検索情報生成部２０６は、機器ＩＤとして、機器ＩＤ管理部２０３から「ＩＤ＿Ｂ」を読み出し、読み出した「ＩＤ＿Ｂ」

を書き込む。コンテンツサーバ検索情報生成部２０６は、中継機器固有情報取得部２０４からルータのＭＡＣアドレスを読み出し、読み出したＭＡＣアドレスを、中継機器固有情報として書き込む。コンテンツサーバ検索情報生成部２０６は、コンテンツサーバ検索パケット３０１のデータサイズがＭＴＵに等しくなるよう、パディングデータを書き込む。ここでは、例としてパディングデータは「０」である。

コンテンツサーバ検索情報生成部２０６は、上記の様に生成したコンテンツサーバ検索パケット３０１を、順次暗号処理部２０２へ出力する。

（７）鍵共有要求情報生成部２０７

鍵共有要求情報生成部２０７は、暗号処理部２０２から、確認パケットを受け取ると、以下に示す様に鍵共有要求パケットを生成する。鍵共有要求パケットは、ＩＰヘッダとＩＰペイロードとから構成される。以下では、暗号処理部２０２から、図４（ｂ）に示した確認パケット３０２を受け取り、図４（ｃ）に示した鍵共有要求パケット３０３を生成する例に基づき説明する。

ＩＰヘッダは、ＤＦビット、ＴＴＬ及び宛先アドレスを含む。鍵共有要求情報生成部２０７は、ＤＦビットを「有効」に設定する。鍵共有要求情報生成部２０７は、ＴＴＬを「１」に設定する。鍵共有要求情報生成部２０７は、宛先アドレスとして、確認パケット３０２のＩＰペイロードからコンテンツサーバ２０のＩＰアドレスを読み出し、当該ＩＰアドレスを書き込む。なお、鍵共有要求情報生成部２０７が設定するＴＴＬは、予めコンテンツサーバ２０から通知されているものとする。

ＩＰペイロードは、パケット種別、機器ＩＤ、中継機器固有情報及びパディングデータを含む。鍵共有要求情報生成部２０７は、当該パケットが、鍵共有要求パケットであることを示すために、パケット種別として「鍵共有要求」を書き込む。鍵共有要求情報生成部２０７は、機器ＩＤとして、機器ＩＤ管理部２０３から、「ＩＤ＿Ｂ」を読み出し、読み出した「ＩＤ＿Ｂ」を書き込む。鍵共有要求情報生成部２０７は、中継機器固有情報取得部２０４からルータのＭＡＣアドレスを読み出し、読み出したＭＡＣアドレスを、中継機器固有情報として書き込む。鍵共有要求情報生成部２０７は、鍵共有要求パケット３０３のデータサイズがＭＴＵに等しくなるよう、パディングデータを書き込む。ここでは、例としてパディングデータは「０」である。

鍵共有要求情報生成部２０７は、上記の様に生成した鍵共有要求パケット３０３を、順次暗号処理部２０２へ出力する。

（８）共有鍵生成部２０８

共有鍵生成部２０８は、予め、外部の管理センタから楕円曲線Ｅと元Ｇとが与えられているものとする。

共有鍵生成部２０８は、鍵共有要求情報生成部２０７により、鍵共有要求パケットが生成され、鍵共有要求パケットが、コンテンツサーバ２０へ送信されると、以下に示す様にして、共有鍵生成処理を行う。

共有鍵生成部２０８は、秘密鍵ｘＢを設定して、次式により公開鍵ＹＢを算出する。

ＹＢ＝ｘＢ＊Ｇ

共有鍵生成部２０８は、算出した公開鍵ＹＢを、コンテンツサーバ２０へ送信すると共に、コンテンツサーバ２０から、コンテンツサーバ２０の公開鍵であるＹＡを受信する。

共有鍵生成部２０８は、自身の秘密鍵と受信したコンテンツサーバ２０の公開鍵ＹＡとから、ｘＢ＊ＹＡを算出することにより共有鍵を生成し、生成した共有鍵を内部に記憶する。

ここで、先程、コンテンツサーバ２０の共有鍵生成部１０８により算出された共有鍵ｘＡ＊ＹＢは、

ｘＡ＊ＹＢ＝（ｘＡ×ｘＢ）＊Ｇ

のように変形できる。

一方、共有鍵生成部２０８により算出された共有鍵ｘＢ＊ＹＡは、

ｘＢ＊ＹＡ＝（ｘＢ×ｘＡ）＊Ｇ

＝（ｘＡ×ｘＢ）＊Ｇ

のように変形できる。

従って、共有鍵生成部１０８により算出された共有鍵ｘＡ＊ＹＢと、共有鍵生成部２０８により算出された共有鍵ｘＢ＊ＹＡとが同じものであることは明らかである。

（９）記憶部２０９

記憶部２０９は、具体的にはハードディスクドライブユニットであり、暗号処理部２０２により復号されたコンテンツを受け取り、受け取ったコンテンツを格納する。

３．端末４０及び端末５０の構成

端末４０及び端末５０は、図１に示す様に、ルータ１２の下に接続された機器である。端末４０及び端末５０は、通信部、暗号処理部、機器ＩＤ管理部、中継機器固有情報取得部、最大伝送量探査部、コンテンツサーバ検索情報生成部、鍵共有要求情報生成部、共有鍵生成部及び記憶部から構成される。

端末４０及び端末５０の構成は、端末３０と同一であり、各構成要素の機能も端末３０の各構成要素と同一であるため、端末４０及び端末５０の機能ブロック図は図示しておらず、説明を省略する。

端末４０及び端末５０は、ＴＴＬを「１」に設定したコンテンツサーバ検索パケットを送信すると、コンテンツサーバ検索パケットは、ルータ１２で破棄され、コンテンツサーバ２０へは到達しない。

ここで、例えば、端末４０及び端末５０が、ＴＴＬを「４」に設定した不正なコンテンツサーバ検索パケットを送出すると、当該コンテンツサーバ検索パケットは、コンテンツサーバ２０へ到達する。しかしながら、コンテンツサーバ２０は、コンテンツサーバ検索パケットを受信すると、ＴＴＬを「１」に設定した確認パケットを送信元端末へ返送するため、結局、当該確認パケットは、端末４０及び端末５０には到達せず、端末４０及び端末５０は、コンテンツサーバ２０のＩＰアドレスを取得することは出来ない。ゆえに、端末４０及び端末５０は、コンテンツサーバ２０と鍵共有処理を行うことが出来ない。

＜動作＞

ここでは、図５から図９に示したフローチャートを用いて、コンテンツ配信システム１の動作について説明する。

（１）全体の動作

先ず、図５に示したフローチャートを用いて、コンテンツ配信システム１全体の動作について説明する。

端末３０において要求が発生すると（ステップＳ１）、コンテンツサーバ２０及

び端末３０の間でＡＤ判定処理を行う（ステップＳ２）。続いて、コンテンツサーバ２０及び端末３０の間で鍵共有処理を行い（ステップＳ３）、コンテンツサーバ２０は、コンテンツ送信処理を行い（ステップＳ４）、端末３０は、コンテンツ受信処理を行う（ステップＳ５）。

なお、図５のフローチャートは、コンテンツサーバ２０及び端末３０の動作のみを記載しているが、端末４０及び端末５０は、端末３０と同様に動作するため、ここでは、説明の便宜上、コンテンツサーバ２０及び端末３０の動作のみを記載している。

（２）ＡＤ判定処理の動作

ここでは、図６及び図７に示したフローチャートを用いて、ＡＤ判定処理の動作について説明する。なお、ここで説明する動作は、図５のステップＳ２の詳細である。

端末３０の中継機器固有情報取得部２０４は、自身が接続されているルータのＭＡＣアドレスを取得する（ステップＳ１１）。コンテンツサーバ検索情報生成部２０６は、ＴＴＬを「１」に設定し、中継機器固有情報として、ステップＳ１１で取得したＭＡＣアドレスを書き込み、ＭＴＵに等しいデータサイズのコンテンツサーバ検索パケットを生成する（ステップＳ１２）。コンテンツサーバ検索情報生成部２０６は、生成したコンテンツサーバ検索パケットを、順次暗号処理部２０２へ出力し、暗号処理部２０２は、コンテンツサーバ検索パケットを受け取り、受け取ったパケットのＩＰペイロードを暗号化する（ステップＳ１３）。通信部２０１は、ＩＰペイロードが暗号化されたコンテンツサーバ検索パケットを、マルチキャスト送信する（ステップＳ１４）。

コンテンツサーバ２０は、端末３０から送信されたコンテンツサーバ検索パケットを受信し（ステップＳ１４）、暗号化されているＩＰペイロードを、暗号処理部１０２により復号する（ステップＳ１５）。ＡＤ判定部１０６は、コンテンツサーバ検索パケットのＩＰペイロードに含まれる送信元端末（端末３０）の機器ＩＤを読む（ステップＳ１６）。ＡＤ判定部１０６は、内部に格納しているＣＲＬを参照し、端末３０の機器ＩＤが、ＣＲＬに記載されているか否か判断し、機器ＩＤがＣＲＬに記載されている場合（ステップＳ１７でＹＥＳ）、コンテンツサーバ２０は

処理を終了する。

機器ＩＤがＣＲＬに記載されていない場合（ステップＳ１７でＮＯ）、ＡＤ判定部１０６は、ＩＰヘッダに含まれるＴＴＬを読む（ステップＳ１８）。ＴＴＬが「１」でない場合（ステップＳ１９でＮＯ）、コンテンツサーバ２０は処理を終了する。

ＴＴＬが「１」の場合（ステップＳ１９でＹＥＳ）、ＡＤ判定部１０６は、ＩＰペイロードに含まれる中継機器固有情報と、中継機器固有情報取得部１０４が記憶している中継機器固有情報とを取得する（ステップＳ２０）。ＡＤ判定部１０６は、両者が一致するか否か判断し、一致しない場合（ステップＳ２１でＮＯ）、コンテンツサーバ２０は処理を終了する。

一致する場合（ステップＳ２１でＹＥＳ）、ＡＤ判定部１０６は、確認情報生成部１０７に確認パケットを生成する指示を出力し、確認情報生成部１０７は、ＴＴＬを「１」に設定し、自身のＩＰアドレスを含む確認パケットを生成し（ステップＳ２２）、生成した確認パケットを暗号処理部１０２へ出力する。暗号処理部１０２は、確認パケットのＩＰペイロードを暗号化し（ステップＳ２３）、通信部１０１は、確認パケットを端末３０へ送信し、端末３０は、確認パケットを受信する（ステップＳ２４）。

端末３０の暗号処理部２０２は、受信した確認パケットのＩＰペイロードを復号し（ステップＳ２５）、確認パケットを鍵共有要求情報生成部２０７へ出力する。鍵共有要求情報生成部２０７は、確認パケットのＩＰペイロードに含まれるコンテンツサーバ２０のＩＰアドレスを宛先アドレスとし、ＴＴＬを「１」に設定し、中継機器固有情報を書き込み、パケットのデータサイズをＭＴＵに設定して鍵共有要求パケットを生成する（ステップＳ２６）。

鍵共有要求情報生成部２０７は、生成した鍵共有要求パケットを暗号処理部２０２へ出力し、暗号処理部２０２は、鍵共有要求パケットのＩＰペイロードを暗号化する（ステップＳ２７）。通信部２０１は、鍵共有要求パケットをコンテンツサーバ２０へ送信し、コンテンツサーバ２０は、鍵共有要求パケットを受信する（ステップＳ２８）。

コンテンツサーバ２０の暗号処理部１０２は、受信した鍵共有要求パケットのＩＰペイロードを復号し（ステップＳ２９）、鍵共有要求パケットをＡＤ判定部１０

６へ出力する。ＡＤ判定部１０６は、鍵共有要求パケットのＩＰペイロードに含まれる端末３０の機器ＩＤを読む（ステップＳ３０）。ＡＤ判定部１０６は、内部に格納しているＣＲＬを参照し、ステップＳ３０で読み出した端末３０の機器ＩＤが、ＣＲＬに記載されているか否か判断し、機器ＩＤがＣＲＬに記載されている場合（ステップＳ３１でＹＥＳ）、コンテンツサーバ２０は処理を終了する。

機器ＩＤがＣＲＬに記載されていない場合（ステップＳ３１でＮＯ）、ＡＤ判定部１０６は、ＩＰヘッダに含まれるＴＴＬを読む（ステップＳ３２）。ＴＴＬが「１」でない場合（ステップＳ３３でＮＯ）、コンテンツサーバ２０は処理を終了する。

ＴＴＬが「１」の場合（ステップＳ３３でＹＥＳ）、ＡＤ判定部１０６は、ＩＰペイロードに含まれる中継機器固有情報と、中継機器固有情報取得部１０４が記憶している中継機器固有情報とを取得する（ステップＳ３４）。ＡＤ判定部１０６は、両者が一致するか否か判断し、一致しない場合（ステップＳ３５でＮＯ）、コンテンツサーバ２０は処理を終了する。一致する場合（ステップＳ３５でＹＥＳ）、コンテンツサーバ２０及び端末３０は、図５のステップＳ３の処理を続ける。

（３）鍵共有処理の動作

ここでは、図８に示したフローチャートを用いて、鍵共有処理の動作について説明する。なお、ここで説明する動作は、図５のステップＳ３の詳細であり、コンテンツサーバ２０の共有鍵生成部１０８及び端末３０の共有鍵生成部２０８で行われる処理である。

コンテンツサーバ２０は、秘密鍵ｘＡを設定し（ステップＳ４１）、一方で、端末３０は、秘密鍵ｘＢを設定する（ステップＳ４２）。

コンテンツサーバ２０及び端末３０は、共に管理センタから、楕円曲線Ｅ：$y = x^3 + ax + b$と、元Ｇとを取得する（ステップＳ４３及びステップＳ４４）。

コンテンツサーバ２０は、公開鍵ＹＡ＝ｘＡ＊Ｇを算出し（ステップＳ４５）、算出した公開鍵ＹＡを端末３０へ送信し、端末３０はコンテンツサーバ２０の公開鍵ＹＡを受信する（ステップＳ４７）。

一方、端末３０は、公開鍵ＹＢ＝ｘＢ＊Ｇを算出し（ステップＳ４６）、算出した公開鍵ＹＢをコンテンツサーバ２０へ送信し、コンテンツサーバ２０は、端末３０の公開鍵ＹＢを受信する（ステップＳ４８）。

コンテンツサーバ２０は、共有鍵ｘＡ＊ＹＢを算出し（ステップＳ４９）、端末３０は、共有鍵ｘＢ＊ＹＡを算出する（ステップＳ５０）。

このとき、コンテンツサーバ２０が算出する共有鍵は、

ｘＡ＊ＹＢ＝（ｘＡ×ｘＢ）＊Ｇと変形できる。

一方、端末３０が算出する共有鍵は、

ｘＢ＊ＹＡ＝（ｘＢ×ｘＡ）＊Ｇ

＝（ｘＡ×ｘＢ）＊Ｇと変形できる。

従って、コンテンツサーバ２０と端末３０とで算出された共有鍵は同一のものであることがわかる。

コンテンツサーバ２０の共有鍵生成部１０８、及び、端末３０の共有鍵生成部２０８は、それぞれ、算出した共有鍵を内部に格納する。続いて、コンテンツサーバ２０は、図５のステップＳ４の処理を続け、端末３０はステップＳ５の処理を続ける。

（４）コンテンツ送信処理の動作

ここでは、図９（ａ）に示したフローチャートを用いてコンテンツ送信処理の動作について説明する。なお、ここで説明する動作は、図５のステップＳ４の詳細である。

共有鍵生成部１０８からの指示を受け、コンテンツ格納部１０９は、内部に格納しているコンテンツを読み出し（ステップＳ６１）、読み出したコンテンツを暗号処理部１０２へ出力する。暗号処理部１０２は、コンテンツを受け取ると、共有鍵生成部１０８から共有鍵「ｘＡ＊ＹＢ」を読み出す（ステップＳ６２）。

暗号処理部１０２は、共有鍵「ｘＡ＊ＹＢ」を暗号鍵として用いてコンテンツを暗号化し、暗号化コンテンツを生成する（ステップＳ６３）。

通信部１０１は、暗号化コンテンツを、端末３０へ送信し（ステップＳ６４）、図５のフローチャートに戻る。

（５）コンテンツ受信処理の動作

ここでは、図９（ｂ）に示したフローチャートを用いてコンテンツ受信処理の動作について説明する。なお、ここで説明する動作は、図５のステップＳ５の詳細である。

端末３０の通信部２０１は、コンテンツサーバ２０から暗号化コンテンツを受信する（ステップＳ７１）。通信部２０１は、受信した暗号化コンテンツを暗号処理部２０２へ出力する。

暗号処理部２０２は、暗号化コンテンツを受け取ると、共有鍵生成部２０８が記憶している共有鍵「ｘＢ＊ＹＡ」を読み出す（ステップＳ７２）。

暗号処理部２０２は、共有鍵「ｘＢ＊ＹＡ」を復号鍵として用い暗号化コンテンツを復号してコンテンツを生成する（ステップＳ７３）。暗号処理部２０２は、復号したコンテンツを記憶部２０９へ格納し（ステップＳ７４）、図５のフローチャートに戻る。

＜変形例１＞

ここでは、コンテンツ配信システム１の第１変形例であるコンテンツ配信システム１ａについて説明する。コンテンツ配信システム１において、ＡＤ内には一つのルータが存在し、ＡＤ内の各機器は、当該一つのルータ下に接続されていた。これに対し、コンテンツ配信システム１ａにおいては、ＡＤ内には複数個のルータが存在し、ＡＤ内の各機器は、複数個のルータを介してコンテンツサーバ２０と接続されている。

以下では、図面を参照して詳細に説明する。

図１０は、コンテンツ配信システム１ａの構成を示す図である。同図に示す様に、コンテンツ配信システム１ａは、ルータ１０、ルータ１１、ルータ１１ａ、ルータ１１ｂ、ルータ１２、コンテンツサーバ２０、端末３０ａ及び端末３０ｂから構成される。インターネット６０に接続されたルータ１０には、ルータ１１及びルータ１２が接続されている。ルータ１１、ルータ１１ａ及びルータ１１ｂは、ＡＤ内に存在する中継機器であり、ルータ１２は、ＡＤ外に存在する中継機器である。

ルータ１１には、コンテンツサーバ２０とルータ１１ａとが接続されており、ルータ１１ａには、端末３０ａとルータ１１ｂとが接続されており、ルータ１１ｂには端末３０ｂが接続されている。ルータ１２には、１以上の端末が接続されているが、ルータ１２に接続されている端末については図示しておらず説明を省略する。

なお、コンテンツ配信システム１ａにおいて、各機器は通信プロトコルとしてＩＰｖ４を使用して通信を行うものとする。

ここで、コンテンツサーバ２０は、第１の実施の形態におけるコンテンツサーバ２０と同一の構成及び機能を有するため説明を省略する。

図１１は、端末３０ｂの構成を機能的に示す機能ブロック図である。同図に示す様に、端末３０ｂは、通信部２０１、暗号処理部２０２、機器ＩＤ管理部２０３、最大伝送量探査部２０５、ＴＴＬ検索部２０６ｂ、鍵共有要求情報生成部２０７、共有鍵生成部２０８及び記憶部２０９から構成される。図１１において、端末３０（図３）と同一の機能を有する構成要素には、図３で用いた符号と同一の符号を付し、説明を省略する。

端末３０ｂは、端末３０と異なり、中継機器固有情報取得部２０４とコンテンツサーバ検索情報生成部２０６とを有しておらず、ＴＴＬ検索部２０６ｂを有する。端末３０ｂは、コンテンツサーバ２０と通信を行うために設定すべきＴＴＬを知る必要があり、ＴＴＬ検索部２０６ｂは、適切なＴＴＬを検索する機能を有する。

ＴＴＬ検索部２０６ｂは、図１２に示すＴＴＬ検索パケット３０４を生成する。同図に示す様に、ＴＴＬ検索パケット３０４は、ＩＰヘッダとＩＰペイロードとから構成され、ＩＰヘッダは、ＤＦビット「有効」、ＴＴＬ「ｎ」及び宛先アドレス「マルチキャストアドレス」を含み、ＩＰペイロードは、パケット種別「ＴＴＬ検索」、機器ＩＤ「ＩＤ＿Ｃ」及びパディングデータ「０」を含む。ここで、「ｎ」は、１≦ｎ＜２５５を満たす整数である。また、「ＩＤ＿Ｃ」は、端末３０ｂを一意に識別する機器ＩＤであり、具体的には機器ＩＤ管理部２０３に記憶されている端末３０ｂに固有の８バイトデータである。なお、端末３０ａは、端末３０ｂと同様の構成及び機能を有するため説明を省略する。

図１３は、コンテンツ配信システム１ａ全体の動作を示すフローチャートである。

端末３０ｂにおいて要求が発生すると（ステップＳ８１）、端末３０ｂは、ＴＴＬ検索処理を行い（ステップＳ８２）、コンテンツサーバ２０と通信を行うために設定すべきＴＴＬを検索する。ＴＴＬが決定すると、コンテンツサーバ２０及び端末３０ｂの間でＡＤ判定処理を行う（ステップＳ８３）。続いて、コンテンツサーバ２０及び端末３０ｂの間で鍵共有処理を行い（ステップＳ８４）、コンテンツサーバ２０は、コンテンツ送信処理を行い（ステップＳ８５）、端末３０ｂは、コンテンツ受信処理を行う（ステップＳ５）。

なお、図１３のフローチャートは、コンテンツサーバ２０及び端末３０ｂの動作のみを記載しているが、端末３０ａは、端末３０ｂと同様に動作するため、ここでは、説明の便宜上コンテンツサーバ２０及び端末３０ｂの動作のみを記載している。

次に、図１４に示したフローチャートを用いて、端末３０ｂがコンテンツサーバ２０と通信を行うために設定すべきＴＴＬを検索する処理の動作について説明する。なお、ここで説明する動作は、図１３に示したフローチャートのステップＳ８２の詳細である。

ＴＴＬ検索部２０６ｂは、先ず、ｎとして１を設定する（ステップＳ９１）。ＴＴＬ検索部２０６ｂは、ＴＴＬ検索パケットのＴＴＬを「ｎ」に設定し、ＴＴＬ検索パケットを生成する。暗号処理部２０２は、生成されたＴＴＬ検索パケットのＩＰペイロードを暗号化して、通信部２０１は、ＴＴＬ検索パケットをマルチキャスト送信する（ステップＳ９２）。

ＴＴＬ検索部２０６ｂは、コンテンツサーバ２０から確認パケットを受信した場合（ステップＳ９３でＹＥＳ）、コンテンツサーバ２０との通信に用いるＴＴＬを「ｎ」に決定し（ステップＳ９４）、処理を終了する。

ＴＴＬ検索部２０６ｂは、コンテンツサーバ２０から確認パケットを受信しない場合（ステップＳ９３でＮＯ）、ｎが２５５より小さい数であるか否か判断する。ｎが２５５以上である場合（ステップＳ９５でＮＯ）には、ＴＴＬ検索部２０６ｂは、コンテンツサーバ２０の検索に失敗したとみなし処理を終了する。

ｎが２５５より小さい場合（ステップＳ９５でＹＥＳ）、ＴＴＬ検索部２０６ｂは、ｎ＝ｎ＋１とし（ステップＳ９６）、ステップＳ８２に戻り処理を続ける。

この様にして、端末３０ｂは、コンテンツサーバ２０からの応答があるまで、ＴＴＬ検索パケットのＴＴＬを１から２５５まで１ずつインクリメントしてＴＴＬ検索パケットを生成し、マルチキャスト送信を続ける。

続いて、図１５及び図１６に示すフローチャートを用いて、ＡＤ判定処理の動作について説明する。なお、ここで説明する動作は、図１３に示したフローチャートのステップＳ８３の詳細である。

端末３０ｂのＴＴＬ検索部２０６ｂは、ＴＴＬ検索パケットを生成し（ステップＳ１０１）、暗号処理部２０２は、生成されたＴＴＬ検索パケットのＩＰペイロー

ドを暗号化する（ステップＳ１０２）。通信部２０１は、ＩＰペイロードが暗号化されたＴＴＬ検索パケットをマルチキャスト送信し、コンテンツサーバ２０の通信部１０１は、ＴＴＬ検索パケットを受信する（ステップＳ１０３）。

暗号処理部１０２は、暗号化されているＩＰペイロードを復号する（ステップＳ１０４）。ＡＤ判定部１０６は、ＴＴＬ検索パケットのＩＰペイロードに含まれる送信元端末（端末３０ｂ）の機器ＩＤを読む（ステップＳ１０５）。ＡＤ判定部１０６は、内部に格納しているＣＲＬを参照し、ステップＳ１０５で読み出した機器ＩＤが、ＣＲＬに記載されているか否か判断し、機器ＩＤがＣＲＬに記載されている場合（ステップＳ１０６でＹＥＳ）、コンテンツサーバ２０は処理を終了する。

機器ＩＤがＣＲＬに記載されていない場合（ステップＳ１０６でＮＯ）、ＡＤ判定部１０６は、確認情報生成部１０７に確認パケットを生成する指示を出力し、確認情報生成部１０７は、ＴＴＬ検索パケットに含まれるＴＴＬと等しいＴＴＬをＩＰヘッダに設定し、自身のＩＰアドレスを含む確認パケットを生成し（ステップＳ１０９）、生成した確認パケットを暗号処理部１０２へ出力する。暗号処理部１０２は、確認パケットのＩＰペイロードを暗号化し（ステップＳ１１０）、通信部１０１は、確認パケットを端末３０ｂへ送信し、端末３０ｂは、確認パケットを受信する（ステップＳ１１１）。

端末３０ｂの暗号処理部２０２は、受信した確認パケットのＩＰペイロードを復号し（ステップＳ１１２）、確認パケットを鍵共有要求情報生成部２０７へ出力する。鍵共有要求情報生成部２０７は、確認パケットのＩＰペイロードに含まれるコンテンツサーバ２０のＩＰアドレスを宛先アドレスとし、ステップＳ９４で決定したｎをＴＴＬに設定し、パケットのデータサイズをＭＴＵに設定して鍵共有要求パケットを生成する（ステップＳ１１３）。

鍵共有要求情報生成部２０７は、生成した鍵共有要求パケットを暗号処理部２０２へ出力し、暗号処理部２０２は、鍵共有要求パケットのＩＰペイロードを暗号化する（ステップＳ１１４）。通信部２０１は、鍵共有要求パケットをコンテンツサーバ２０へ送信し、コンテンツサーバ２０は、鍵共有要求パケットを受信する（ステップＳ１１５）。

コンテンツサーバ２０の暗号処理部１０２は、受信した鍵共有要求パケットのＩ

Ｐペイロードを復号し（ステップＳ１１６）、鍵共有要求パケットをＡＤ判定部１０６へ出力する。ＡＤ判定部１０６は、鍵共有要求パケットのＩＰペイロードに含まれる端末３０ｂの機器ＩＤを読む（ステップ１１７）。ＡＤ判定部１０６は、内部に格納しているＣＲＬを参照し、端末３０ｂの機器ＩＤが、ＣＲＬに記載されているか否か判断し、機器ＩＤがＣＲＬに記載されている場合（ステップＳ１１８でＹＥＳ）、コンテンツサーバ２０は処理を終了する。

機器ＩＤがＣＲＬに記載されていない場合（ステップＳ１１８でＮＯ）、コンテンツサーバ２０及び端末３０ｂは、図１３のステップＳ８４の処理を続ける。

図１３のステップＳ８４の詳細は、図８に示したフローチャートと同一の処理であり、ステップＳ８５の詳細は、図９（ａ）に示したフローチャートと同一の処理であり、ステップＳ８６の詳細は、図９（ｂ）に示したフローチャートと同一の処理であるため、説明を省略する。

＜変形例２＞

ここでは、コンテンツ配信システム１の第２変形例として、コンテンツ配信システム１ｂについて説明する。

コンテンツ配信システム１ｂは、ＡＤ判定処理の後に鍵共有処理を行うのではなく、鍵共有処理において各機器がＴＴＬを「１」に設定したパケットを送受信することで、鍵共有処理とＡＤ判定処理とを同時に行うシステムである。以下では、図面を参照して詳細に説明する。

図１７は、コンテンツ配信システム１ｂの構成を示す図である。コンテンツ配信システム１ｂは、ルータ１０、ルータ１１、ルータ１２、コンテンツサーバ２０ｂ、端末３０ｃ、端末４０及び端末５０から構成される。ルータ１０、ルータ１１、ルータ１２、端末４０及び端末５０は、コンテンツ配信システム１（図１）と同一の構成及び機能を有するためコンテンツ配信システム１と同一の符号を付して説明を省略する。ここでは、コンテンツ配信システム１と異なる構成及び機能を有するコンテンツサーバ２０ｂ及び端末３０ｃについて説明する。

図１８は、コンテンツサーバ２０ｂの構成を機能的に示す機能ブロック図である。同図に示す様に、コンテンツサーバ２０ｂは、通信部１０１、暗号処理部１０２、機器ＩＤ管理部１０３、最大伝送量探査部１０５、ＡＤ判定部１０６ｂ、共有鍵生

成部１０８ｂ及びコンテンツ格納部１０９から構成される。なお、図１８において、コンテンツサーバ２０（図２）と同一の機能を有する構成要素には、同一の符号を付して説明を省略する。

ＡＤ判定部１０６ｂは、端末３０ｃから受信する公開鍵パケットに含まれるＴＴＬを読み、ＴＴＬが「１」であり、確かにＡＤ内の端末から送信されたパケットであるか否かを判定する。端末３０ｃから受信する公開鍵パケットについては後述する。

共有鍵生成部１０８ｂは、コンテンツサーバ２０の共有鍵生成部１０８と同様に、予め、外部の管理センタから楕円曲線Ｅ：$y=x^3+ax+b$と元Ｇとが与えられている。共有鍵生成部１０８ｂは、秘密鍵ｘＡを設定して公開鍵ＹＡ＝ｘＡ＊Ｇを算出する。共有鍵生成部１０８ｂは、算出した公開鍵ＹＡを分割して公開鍵パケットを生成する。共有鍵生成部１０８ｂは、生成した公開鍵パケットを、暗号処理部１０２及び通信部１０１を介して順次端末３０ｃへ送信する。

コンテンツサーバ２０ｂが生成する公開鍵パケットの一例として、公開鍵パケット３０５のデータ構造を図２０（ａ）に示す。同図に示す様に、公開鍵パケット３０５は、ＩＰヘッダとＩＰペイロードとから構成され、ＩＰヘッダは、ＤＦビット「有効」、ＴＴＬ「１」及び宛先アドレス「端末３０ｃ」を含み、ＩＰペイロードは、パケット種別「公開鍵」、機器ＩＤ「ＩＤ＿Ａ」、公開鍵「ＹＡ」及びパディングデータ「０」を含む。

共有鍵生成部１０８ｂは、ＤＦビットを「有効」に設定することにより、カプセル化を抑止し、ＴＴＬを「１」に設定することにより、公開鍵パケット３０５が、ルータ１１を超えてＡＤ外へ送信されることを抑止する。また、共有鍵生成部１０８ｂは、宛先アドレスに端末３０ｃのＩＰアドレスを設定するが、当該ＩＰアドレスは、コンテンツサーバ２０ｂが既知であるとする。

同図に示す様に、公開鍵パケット３０５のデータサイズは、ＭＴＵに等しい。共有鍵生成部１０８ｂは、最大伝送量探査部１０５からＭＴＵを取得し、取得したＭＴＵに等しくなるようにパディング処理を施して、ＭＴＵに等しいデータサイズの公開鍵パケット３０５を生成する。また、公開鍵パケット３０５のＩＰペイロードは、暗号処理部１０２により暗号化されて、端末３０ｃへ送信される。

共有鍵生成部１０８ｂは、端末３０ｃから通信部１０１と暗号処理部１０２とを介して公開鍵パケットを受け取り、受け取った公開鍵パケットを蓄積して公開鍵ＹＢを生成する。共有鍵生成部１０８ｂは、自身の秘密鍵ｘＡと受信した端末３０ｃの公開鍵ＹＢとから、ｘＡ＊ＹＢを算出することにより共有鍵ｘＡ＊ＹＢを生成し、生成した共有鍵ｘＡ＊ＹＢを内部に記憶する。

共有鍵生成部１０８ｂは、共有鍵ｘＡ＊ＹＢを生成して記憶すると、コンテンツ格納部１０９に対して、コンテンツを読み出す指示を出力する。

図１９は、端末３０ｃの構成を機能的に示す機能ブロック図である。同図に示す様に、端末３０ｃは、通信部２０１、暗号処理部２０２、機器ＩＤ管理部２０３、最大伝送量探査部２０５、共有鍵生成部２０８ｃ及び記憶部２０９から構成される。

図１９において、端末３０（図３）と同一の機能を有する構成要素には、図３で用いた符号と同一の符号を付して説明を省略する。端末３０ｃは、端末３０と異なり、中継機器固有情報取得部２０４、コンテンツサーバ検索情報生成部２０５及び鍵共有要求情報生成部２０６を有していない。

共有鍵生成部２０８ｃは、端末３０の共有鍵生成部２０８と同様に、予め、外部の管理センタから楕円曲線Ｅ：$y = x^3 + ax + b$と元Ｇとが与えられている。

共有鍵生成部２０８ｃは、秘密鍵ｘＢを設定して、公開鍵ＹＢ＝ｘＢ＊Ｇを算出する。共有鍵生成部２０８ｃは、算出した公開鍵ＹＢをパケットに分割して公開鍵パケットを生成し、生成した公開鍵パケットを、暗号処理部２０２及び通信部２０１を介して順次コンテンツサーバ２０ｂに送信する。

端末３０ｃが生成する公開鍵パケットの一例として、公開鍵パケット３０６のデータ構造を図２０（ｂ）に示す。同図に示す様に、公開鍵パケット３０６は、ＩＰヘッダとＩＰペイロードとから構成され、ＩＰヘッダは、ＤＦビット「有効」、ＴＴＬ「１」及び宛先アドレス「コンテンツサーバＩＰアドレス」を含み、ＩＰペイロードは、パケット種別「公開鍵」、機器ＩＤ「ＩＤ＿Ｍ」、公開鍵「ＹＢ」及びパディングデータ「０」を含む。ここで、「ＩＤ＿Ｍ」は、端末３０ｃを一意に識別するために用いられる８バイトデータである。

共有鍵生成部２０８ｂは、ＤＦビットを「有効」に設定することにより、カプセル化を抑止し、ＴＴＬを「１」に設定することにより、公開鍵パケット３０６が、

ルータ１１を超えてＡＤ外へ送信されることを抑止する。また宛先アドレスとして設定するのはコンテンツサーバ２０ｃのＩＰアドレスであり、当該ＩＰアドレスは予め端末３０ｃが既知であるとする。

同図に示す様に、公開鍵パケット３０６のデータサイズは、ＭＴＵに等しい。共有鍵生成部２０８ｂは、最大伝送量探査部２０５からＭＴＵを取得して、取得したＭＴＵに等しいデータサイズにパディング処理を施して、公開鍵パケット３０６を生成する。また、公開鍵パケット３０６のＩＰペイロードは、暗号処理部２０２により暗号化されて、コンテンツサーバ２０ｂへ送信される。

共有鍵生成部２０８ｃは、コンテンツサーバ２０ｂから通信部２０１と暗号処理部２０２とを介して公開鍵パケットを受け取り、受け取った公開鍵パケットを蓄積して公開鍵ＹＡを生成する。

共有鍵生成部２０８は、自身の秘密鍵ｘＢと受信したコンテンツサーバ２０ｂの公開鍵ＹＡとから、ｘＢ＊ＹＡを算出することにより共有鍵を生成し、生成した共有鍵ｘＢ＊ＹＡを内部に記憶する。

次に、図２１及び図２２に示したフローチャートを用いて、コンテンツ配信システム１ｂの動作について説明する。

図２１は、コンテンツ配信システム１ｂの全体の動作を示すフローチャートである。端末３０ｃで要求が発生すると（ステップＳ２０１）、コンテンツサーバ２０ｂと端末３０ｃとの間で鍵共有処理を行う（ステップＳ２０２）。続いて、コンテンツサーバ２０ｂは、コンテンツ送信処理（ステップＳ２０３）を行い、端末３０ｃは、コンテンツ受信処理を行う（ステップＳ２０４）。

図２２は、鍵共有処理の動作を示すフローチャートである。なお、ここに示す動作は、図２１に示したフローチャートのステップＳ２０２の詳細である。

コンテンツサーバ２０ｂは、秘密鍵ｘＡを設定し（ステップＳ２１１）、一方で、端末３０ｃは、秘密鍵ｘＢを設定する（ステップＳ２１２）。

コンテンツサーバ２０ｂ及び端末３０ｃは、共に管理センタから、楕円曲線Ｅ：$y = x^3 + ax + b$と元Ｇとを取得する（ステップＳ２１３及びステップＳ２１４）。

コンテンツサーバ２０ｂは、公開鍵ＹＡ＝ｘＡ＊Ｇを算出する（ステップＳ２１５）。コンテンツサーバ２０ｂは、算出した公開鍵ＹＡを分割して、図２０（ａ）

に示す様に、ＩＰヘッダのＴＴＬを「１」に設定した公開鍵パケットを生成する（ステップＳ２１７）。コンテンツサーバ２０ｂは、生成した公開鍵パケットを順次端末３０ｃへ送信し、端末３０ｃは、公開鍵パケットを受信する（ステップＳ２１９）。

端末３０ｃは、公開鍵ＹＢ＝ｘＢ＊Ｇを算出する（ステップＳ２１６）。端末３０ｃは、算出した公開鍵ＹＢを分割して、図２０（ｂ）に示す様に、ＩＰヘッダのＴＴＬを「１」に設定した公開鍵パケットを生成する（ステップＳ２１８）。端末３０ｃは、生成した公開鍵パケットを順次コンテンツサーバ２０ｂへ送信し、コンテンツサーバ２０ｂは、公開鍵パケットを受信する（ステップＳ２２０）。

コンテンツサーバ２０ｂは、受信した公開鍵パケットに含まれるＴＴＬを確認し（ステップＳ２２１）、確かにＴＴＬが「１」である場合（ステップＳ２２３でＹＥＳ）、ステップＳ２１１で設定した秘密鍵ｘＡと、受信した公開鍵ＹＢとから、共有鍵ｘＡ＊ＹＢを算出する（ステップＳ２２５）。ＴＴＬが「１」でない場合（ステップＳ２２３でＮＯ）、コンテンツサーバ２０ｂは処理を終了する。

端末３０ｃは、ステップＳ２１９で受信した公開鍵パケットに含まれるＴＴＬを確認し（ステップＳ２２２）、確かにＴＴＬが「１」である場合（ステップＳ２２４でＹＥＳ）、ステップＳ２１２で設定した秘密鍵ｘＢと、受信した公開鍵ＹＡとから、共有鍵ｘＢ＊ＹＡを算出する（ステップＳ２２６）。ＴＴＬが「１」でない場合（ステップＳ２２４でＮＯ）、端末３０ｃは処理を終了する。

このとき、コンテンツサーバ２０ｂが算出する共有鍵は、

ｘＡ＊ＹＢ＝（ｘＡ×ｘＢ）＊Ｇと変形できる。

一方、端末３０ｃが算出する共有鍵は、

ｘＢ＊ＹＡ＝（ｘＢ×ｘＡ）＊Ｇ

＝（ｘＡ×ｘＢ）＊Ｇと変形できる。

従って、コンテンツサーバ２０ｂと端末３０ｃとで算出された共有鍵は同一のものであることがわかる。

コンテンツサーバ２０ｂの共有鍵生成部１０８ｂ、及び、端末３０ｃの共有鍵生成部２０８ｃは、それぞれ、算出した共有鍵を内部に格納する。続いて、コンテンツサーバ２０ｂは、図２１のステップＳ２０３の処理を続け、端末３０ｃはステップＳ２０４の処理を続ける。

なお、ステップＳ２０３のコンテンツ送信処理は、コンテンツ配信システム１におけるコンテンツ送信処理の動作（図９（ａ））と同一であるため、説明を省略する。同様に、ステップＳ２０４のコンテンツ受信処理は、コンテンツ配信システム１におけるコンテンツ受信処理の動作（図９（ｂ））と同一であるため、説明を省略する。

＜まとめ＞

以上まとめると、上記第１の実施の形態において、コンテンツサーバ２０は、端末とのデータ通信における隔たりの量を示す通信距離として、端末から受信するパケットに設定されたＴＴＬを用いて、前記端末がＡＤ内の端末であるか、又は、ＡＤ外の端末であるか判定する。

コンテンツ配信システム１において、各端末は、ＴＴＬが「１」であるコンテンツサーバ検索パケットをマルチキャスト送信する。コンテンツサーバ検索パケットは、各端末が接続されているルータを越えて他のサブネットワークへ送信されない。そのため、コンテンツサーバ２０は、自身と同じルータ下に接続されている端末３０から送信されたコンテンツサーバ検索パケットのみを受信する。

コンテンツサーバ２０は、コンテンツサーバ検索パケットを受信すると、ＴＴＬが「１」である確認パケットを返送する。確認パケットは、コンテンツサーバ２０が接続されているルータを越えて他のサブネットワークへ送信されない。そのため、端末４０及び端末５０が、不正に確認パケットを受信することは出来ず、確かに同じルータ下に接続されている端末３０のみが確認パケットが受信することができる。

また、コンテンツサーバ２０と端末３０とは、ＤＦビットを「有効」に設定し、且つ、ＭＴＵに等しいデータサイズにパディング処理を施したパケットを送受信することで伝送経路上の他の端末、特に不正な端末によりＩＰパケットに不必要な情報が付加されて、不正な端末へパケットが転送されるのを抑止する。

また、端末３０は、パケットのＩＰペイロードに自身が接続されているルータのＭＡＣアドレスを包含して送信することにより、コンテンツサーバ２０は、端末３０が確かに自身と同じルータに接続されていることを確認することができる。

上記第１変形例において、コンテンツサーバ２０ａと端末３０とは、複数個の中継機器を介して接続されている。端末３０は、コンテンツサーバ２０ａから応答が

あるまで、ＴＴＬを最小値の「１」から１ずつ増加させたＴＴＬ検索パケットをマルチキャスト送信する。端末３０は、ＴＴＬを「ｎ」に設定したＴＴＬ検索パケットをマルチキャスト送信した後、コンテンツサーバ２０から確認パケットを受信した場合、コンテンツサーバ２０ａと通信を行うために必要な最小のＴＴＬは「ｎ」であると判断する。以後、端末３０とコンテンツサーバ２０ａとは、ＴＴＬを「ｎ」に設定したパケットを送受信することにより、鍵共有処理及びコンテンツ送受信処理を行う。

上記第２変形例において、コンテンツ配信システム１ｂは、コンテンツサーバ２０ｂ及び端末３０ｃが、共に互いのＩＰアドレスを既知である場合に、コンテンツ配信システム１で行うコンテンツサーバ検索処理を省略し、更に、鍵共有処理で送受信する公開鍵パケットのＴＴＬを「１」に設定することで、公開鍵を交換しながらＡＤ判定処理を行うことだ可能なシステムである。

なお、上記第２変形例において、公開鍵パケットに設定されるＴＴＬは必ずしも「１」である必要はない。例えば、コンテンツサーバ２０ｂと端末３０ｃとの間で任意の「ｎ」をＴＴＬに設定し、双方が受信したパケットのＴＴＬが「ｎ」以下であることを確認することによりＡＤ判定を行ってもよい。

また、図２２のステップＳ２２２及びステップＳ２２４の処理は、必ずしも必要ではない。コンテンツサーバ２０ｂのみが、受信したパケットのＴＴＬが「１」であることを確認する構成であってもよい。

更に、第２変形例において、コンテンツサーバ２０ｂのＡＤ判定部１０６ｂは、内部にＣＲＬを格納しており、端末３０ｃから受信する公開鍵パケットに含まれる端末３０ｃの機器ＩＤを読み、読み出した機器ＩＤが、ＣＲＬに含まれるか否か判定してもよい。上記判定により端末３０ｃの機器ＩＤが、ＣＲＬに含まれる場合には、コンテンツサーバ２０ｂは、公開鍵パケットの送信処理を抑制するように構成されてもよい。

≪第２の実施の形態≫

本発明に係る第２の実施の形態として、コンテンツ配信システム２について、図面を参照して説明する。コンテンツ配信システム２は、コンテンツ配信システム１と同様に、端末から送信されるパケットに含まれるＴＴＬを用いて、前記端末がＡ

Ｄ内の端末であるか否かを判定する。コンテンツ配信システム１は、ＡＤ内の端末であると判定された端末とサーバとが鍵を共有する構成を有していたが、コンテンツ配信システム２は、ＡＤ内の端末であると判定された端末を、サーバがグループに登録する構成を有する。

なお、コンテンツ配信システム２において、各機器は通信プロトコルとしてＩＰｖ４を使用して通信を行うものとする。

＜構成＞

図２３は、コンテンツ配信システム２の構成を示す図である。コンテンツ配信システム２は、ルータ１０、ルータ１１、ルータ１２、コンテンツサーバ２０ａ、端末３０、端末４０及び端末５０から構成される。ルータ１０、ルータ１１、ルータ１２、端末３０、端末４０及び端末５０は、コンテンツ配信システム１（図１）と同一の構成及び機能を有するためコンテンツ配信システム１と同一の符号を付して説明を省略する。ここでは、コンテンツ配信システム１と異なる機能を有するコンテンツサーバ２０ａについて説明する。

図２４は、コンテンツサーバ２０ａの構成を示すブロック図である。同図に示す様に、コンテンツサーバ２０ａは、通信部１０１、暗号処理部１０２、機器ＩＤ管理部１０３、中継機器固有情報取得部１０４、最大伝送量探査部１０５、ＡＤ判定部１０６、確認情報生成部１０７、グループ管理部１０８ａ及びコンテンツ格納部１０９から構成される。なお、図２４において、コンテンツサーバ２０（図２）と同一の機能を有する構成要素には、同一の符号を付し、説明を省略する。

グループ管理部１０８ａは、ＡＤ判定部１０６によりＡＤ内の端末であると判定された端末、即ち、グループ内端末の情報を管理する。より具体的には、グループ管理部１０８ａは、ＡＤ判定部１０６から指示を受け、コンテンツ要求ＩＤを生成する。グループ管理部１０８ａは、生成したコンテンツ要求ＩＤを、グループ内端末に送信する。また、グループ管理部１０８ａは、生成した前記コンテンツ要求ＩＤと前記グループ内端末の機器ＩＤとを対応付けて、図２５に示すグループテーブル３５０に登録する。

図２５に示したグループテーブル３５０は、ＡＤ判定部１０６によりＡＤ内の端末であると判定された全ての端末について、機器ＩＤとコンテンツ要求ＩＤとが対

応付けられて構成されており、例えば、機器ＩＤ「ＩＤ＿Ｅ」に対応付けられているコンテンツ要求ＩＤは、「ＣＩＤ＿０００１」である。同様に、機器ＩＤ「ＩＤ＿Ｆ」に対応付けられているコンテンツ要求ＩＤは、「ＣＩＤ＿０００２」である。

また、グループ管理部１０８ａは、端末から、当該端末の機器ＩＤと当該端末が有するコンテンツ要求ＩＤとを含むコンテンツ送信要求を受け付けると、前記機器ＩＤと前記コンテンツ要求ＩＤとがグループテーブル３５０に登録されているか否か判断する。

グループ管理部１０８ａは、前記機器ＩＤと前記コンテンツ要求ＩＤとがグループテーブル３５０に登録されていると判断すると、コンテンツ格納部１０９からコンテンツを読み出し、読み出したコンテンツを通信部１０１を介して端末へ送信する。

＜動作＞

図２６（ａ）及び図２６（ｂ）に示すフローチャートを用いて、コンテンツ配信システム２の動作について説明する。なお、図２６（ａ）及び図２６（ｂ）のフローチャートは、コンテンツサーバ２０ａ及び端末３０の動作のみを記載しているが、端末４０及び端末５０は、端末３０と同様に動作するため、ここでは、コンテンツサーバ２０ａ及び端末３０の動作のみを記載している。

図２６（ａ）は、コンテンツ配信システム２におけるグループ登録処理の動作を示すフローチャートである。

先ず、端末３０で要求が発生すると（ステップＳ１３１）、コンテンツサーバ２０ａと端末３０との間でＡＤ判定処理を行う（ステップＳ１３２）。なお、ステップＳ１３２の詳細は、図６及び図７に示した動作と同一であるので説明は省略する。

続いて、コンテンツサーバ２０ａは、コンテンツ要求ＩＤを生成し（ステップＳ１３３）、生成したコンテンツ要求ＩＤを端末３０へ送信し、端末３０は、コンテンツ要求ＩＤを受信する（ステップＳ１３４）。

コンテンツサーバ２０ａのグループ管理部１０８ａは、ステップＳ１３３で生成したコンテンツ要求ＩＤと、端末３０の機器ＩＤとを対応付けてグループテーブル３５０に登録する（ステップＳ１３５）。端末３０は、ステップＳ１３４で受信したコンテンツ要求ＩＤを、機器ＩＤ管理部２０３に格納する（ステップＳ１３６）。

図２６（ｂ）は、コンテンツ配信システム２における、コンテンツ要求処理の動作を示すフローチャートである。

先ず、端末３０で要求が発生すると（ステップＳ１４１）、機器ＩＤ管理部２０３は、内部に格納している機器ＩＤとコンテンツ要求ＩＤとを読み出し（ステップＳ１４２）、通信部２０１を介して読み出した機器ＩＤとコンテンツ要求ＩＤとをコンテンツサーバ２０ａへ送信する（ステップＳ１４３）。コンテンツサーバ２０ａの通信部１０１は、端末３０から送信された機器ＩＤとコンテンツ要求ＩＤとを受信する（ステップＳ１４３）。

コンテンツサーバ２０ａのグループ管理部１０８ａは、内部に格納しているグループテーブル３５０を読み出し（ステップＳ１４４）、ステップＳ１４３にて端末３０から受信した機器ＩＤとコンテンツ要求ＩＤとが、グループテーブル３５０に登録されているか否か判断する。

機器ＩＤとコンテンツ要求ＩＤとがグループテーブル３５０に登録済みである場合（ステップＳ１４５でＹＥＳ）、グループ管理部１０８ａは、コンテンツ格納部１０９からコンテンツを読み出す（ステップＳ１４６）。グループ管理部１０８ａは、読み出したコンテンツを通信部１０１を介して端末３０へ送信し、端末３０は、コンテンツを受信する（ステップＳ１４７）。端末３０は、受信したコンテンツを再生するか、又は、記憶部２０９へ格納する（ステップＳ１４８）。

機器ＩＤとコンテンツ要求ＩＤとが登録済みでない場合（ステップＳ１４５でＮＯ）、コンテンツサーバ２０ａは処理を終了する。

＜まとめ＞

第２の実施の形態をまとめると、通信装置と他の通信装置とのデータ通信における隔たりの量を示す通信距離を取得する取得手段と、取得した前記通信距離が、所定値以下であるか否か判定する判定手段と、前記判定の結果が肯定的である場合に、前記他の通信装置をグループに登録する登録手段とを備えることを特徴とする通信装置である。

前記通信手段は、前記他の通信装置とデータの通信を行い、前記取得手段は、前記他の通信装置から送信されたデータを当該通信装置が受信するまでの間に、前記データが経由した中継機器の数を示す前記通信距離を取得することを特徴とする。

前記取得手段は、前記他の通信装置から送信されたデータを当該通信装置が受信するまでの間に、前記データが経由した中継機器の数として、前記データが経由したルータの数を示す前記通信距離を取得することを特徴とする。

前記通信手段は、ルータを一つ経由する毎に１ずつ値が減少する性質を有するＴＴＬを含むパケットの形式で、前記データの通信を行い、前記取得手段は、前記通信手段が受信するパケットに含まれる前記ＴＴＬを用いて、前記データが経由したルータの数を示す前記通信距離を取得することを特徴とする。

前記通信手段は、前記他の通信装置から、当該他の通信装置が接続されている第１のルータを一意に識別する第１識別情報を含む前記パケットを受信し、前記通信装置は、更に、当該通信装置が接続されている第２のルータを一意に識別する第２識別情報を取得するルータ情報取得手段と、前記第１識別情報と前記第２識別情報とが一致するか否か判断する判断手段と、前記判断手段による判断の結果が否定的である場合に、前記通信手段による前記コンテンツの送受信を抑制する抑制手段とを備えることを特徴とする。

前記通信手段が送受信する各パケットは、当該通信手段が接続されているネットワークの最大伝送量（Maximum Transmission Unit）に等しいデータサイズであり、且つ、分割して送受信することが禁止されていることを特徴とする。

前記通信手段は、前記他の通信装置から、送信時に所定ＴＴＬが設定されて送信されたパケットを受信し、前記取得手段は、前記通信手段が受信した前記パケットからＴＴＬを読み、読み出したＴＴＬと前記所定ＴＴＬとの差分である前記通信距離を取得することを特徴とする。

前記通信手段は、前記他の通信装置から、送信時に前記所定ＴＴＬとして「１」が設定されて送信された前記パケットを受信することを特徴とする。

前記通信機器は、前記登録手段によりグループに登録された他の通信機器に対してコンテンツを送信するコンテンツ送信手段を備えることを特徴とする。

また、第２の実施の形態は、第１の通信機器と、１以上の中継機器を介して接続された第２の通信機器とから構成されるグループ登録システムであって、前記第１の通信機器から登録要求を受け付けると、前記第２の通信機器とのデータ通信における隔たりの量を示す通信距離を取得する取得手段と、取得した前記通信距離が、

所定値以下であるか否か判定する判定手段と、前記判定の結果が肯定的である場合に、前記第２の通信機器をグループに登録する登録手段を備え、前記第２の通信機器は、前記第１の通信機器に対して登録要求を送信することを特徴とする。

≪その他の変形例≫

なお、本発明を上記第１の実施の形態、その変形例及び第２の実施の形態に基づき説明してきたが、本発明がこれらの実施形態に限定されないのは勿論であり、以下の様な場合も本発明に含まれる。

（１）上記実施の形態では、コンテンツサーバは、前記端末から受信するパケットに含まれるＴＴＬを用いて、ＡＤ内の端末であるか、又は、ＡＤ外の端末であるか判定しているが、コンテンツサーバにおけるＡＤ判定方法は、これに限定されない。例えば、コンテンツサーバは、コンテンツサーバと端末との長さを測定し、測定した長さに基づきＡＤ判定してもよい。また、コンテンツサーバは、コンテンツサーバと端末との間の通信に要する時間を測定し、測定した時間に基づきＡＤ判定してもよい。なお、これらの測定方法については限定されない。

（２）上記実施の形態において、コンテンツ配信システムに含まれる各機器は、ＩＰｖ４のプロトコルで通信を行う構成を有しているが、本発明において、通信プロトコルはＩＰｖ４に限定されないのは勿論である。例えば、ＩＰｖ６のプロトコルで通信を行う構成も本発明に含まれる。この場合、ＩＰｖ４のＴＴＬフィールドに替えて、ＩＰｖ６のＨｏｐ　Ｌｉｍｉｔフィールドを利用してＡＤ判定を行ってもよい。

（３）上記第１の実施の形態では、各機器は、ＴＴＬが「１」であるパケットを送受信する構成を有しているが、本発明において、ＴＴＬフィールドに設定するＴＴＬは「１」に限定されないのは勿論である。

第１の実施の形態においては、例えば、コンテンツサーバと端末との間で所定のＴＴＬ値（ここでは１０とする）をＴＴＬフィールドに設定するように予め決めておく。端末は、ＴＴＬを「１０」に設定したコンテンツサーバ検索パケットをマルチキャスト送信する。コンテンツサーバは、コンテンツサーバ検索パケットを受信すると、ＴＴＬフィールドに含まれるＴＴＬが所定値「１０」からの増減が無いか、を確認しＴＴＬが「１０」である場合に、当該端末と鍵共有処理を行うように構成

してもよい。

（４）上記実施の形態において、端末３０はルータ１１に直接接続される構成を有しているが、本発明はこの構成に限定されず、例えば、端末３０とルータ１１とがスイッチやハブなどを介して接続される構成も本発明に含まれる。

（５）上記実施の形態では、ＩＰパケットの送信時と受信時とにおける、ＴＴＬの減少量が「０」の場合をＡＤ内と判定しているが、例えばＩＰパケットの送信時と受信時とにおけるＴＴＬの減少量が「所定値以下」の場合をＡＤ内と判定することでＡＤを任意に広げることが可能である。例えば、ＴＴＬの減少量が「２」である端末までＡＤ内端末であるとすることもできる。

（６）上記第１の実施の形態及びその変形例において、コンテンツサーバから暗号化コンテンツを受信した端末は、前記暗号化コンテンツを復号した後、記憶部に格納する構成を有しているが、端末は、復号したコンテンツを再生する構成も本発明に含まれる。

（７）上記実施の形態において、ＩＰパケットのＩＰペイロードを暗号化したり復号したりするときに暗号処理部で用いる暗号鍵は、グローバルシークレットな値としているが、必ずしもこれに限定されず、例えば事前にゼロ知識証明を利用したチャレンジ－レスポンス型のハンドシェイクを行い、セッション鍵を共有する方法であってもよい。

（８）上記実施の形態において、各機器は、ＭＴＵに等しいデータサイズのパケットを送受信する構成を有しているが、各機器は、必ずしもＭＴＵに等しいデータサイズのパケットを送受信する必要は無く、データサイズがＭＴＵと異なるパケットを送受信する構成も本発明に含まれる。

（９）上記実施の形態において、各機器は、ＤＦビットを「有効」に設定したパケットを送受信する構成を有しているが、各機器は、必ずしもＤＦビットを「有効」に設定したパケットを送受信する必要は無く、ＤＦビットが「無効」の場合であっても本発明に含まれる。

（１０）上記実施の形態において、各機器は、自身が接続されている中継機器を識別する中継機器固有情報を取得し、取得した中継機器固有情報を含むパケットを送信する構成を有しているが、各機器は、必ずしも中継機器固有情報を含んだパケ

ットを送信する必要は無い。各機器は、中継機器固有情報を含まないパケットを送受信する構成も本発明に含まれる。

（１１）上記の実施の形態では、端末の機器ＩＤをグループテーブルに登録する構成を有しているが、本発明は、これに限定されず、例えば、端末に装着して用いるメモリカードなどの記録媒体のＩＤをグループテーブルに登録するような場合も含まれる。

（１２）また、本発明は、コアＣＰＵとＤＳＰとにより構成されるシステムＬＳＩであってもよい。前記システムＬＳＩが、ＤＰＳプログラムであるコンテンツ配信プログラムを実行する構成も本発明に含まれる。

（１３）本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるディジタル信号であるとしてもよい。

また、本発明は、前記コンピュータプログラム又は前記ディジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フロッピーディスク、ハードディスク、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤ、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ、ＢＤ（Ｂｌｕ－ｒａｙ　Ｄｉｓｃ）、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記ディジタル信号であるとしてもよい。

また、本発明は、前記コンピュータプログラム又は前記ディジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク等を経由して伝送するものとしてもよい。

また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。

また、前記プログラム又は前記ディジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記ディジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

（１４）上記実施の形態及び上記変形例をそれぞれ組み合わせる構成も本発明に

含まれる。

産業上の利用の可能性

上記において説明したコンテンツ配信システムは、映画、音楽などのディジタル化された著作物を、放送やネットワークなどを介して流通させる産業において、家庭内においては自由にコンテンツを利用し、家庭外にはコンテンツの流出を防ぐ仕組みとして利用できる。

請　求　の　範　囲

1．通信装置であって、以下を含む：

・取得手段、

当該通信装置と他の通信装置とのデータ通信における隔たりの量を示す通信距離を取得する；

・判定手段、

取得した前記通信距離が、所定値以下であるか否か判定する；

・通信手段、

前記判定の結果が肯定的である場合に、前記他の通信装置との間でコンテンツの送信又は受信を行う。

2．前記通信手段は、前記コンテンツの送信又は受信に先立ち、前記他の通信装置とデータの通信を行い、

前記取得手段は、前記他の通信装置から送信されたデータを当該通信装置が受信するまでの間に、前記データが経由した中継機器の数を示す前記通信距離を取得する

ことを特徴とする請求の範囲１に記載の通信装置。

3．前記取得手段は、前記他の通信装置から送信されたデータを当該通信装置が受信するまでの間に、前記データが経由した中継機器の数として、前記データが経由したルータの数を示す前記通信距離を取得する

ことを特徴とする請求の範囲２に記載の通信装置。

4．前記通信手段は、ルータを一つ経由する毎に１ずつ値が減少する性質を有するＴＴＬ（Time To Live）を含むパケットの形式で、前記データの通信を行い、

前記取得手段は、前記通信手段が受信するパケットに含まれる前記ＴＴＬを用いて、前記データが経由したルータの数を示す前記通信距離を取得する

ことを特徴とする請求の範囲３に記載の通信装置。

5．請求の範囲４に記載の通信装置は、更に、以下を備える：

・鍵共有手段、

前記他の通信装置と鍵情報を共有する。

6．請求の範囲５に記載の通信装置は、更に、以下を備え：

・暗号処理手段、

前記鍵共有手段により前記他の通信装置と共有した前記鍵情報を用いて、前記コンテンツの暗号化処理及び暗号化された前記コンテンツの復号処理を行う；

前記通信手段は、前記他の通信装置との間で、前記暗号処理手段により暗号化された前記コンテンツの送信又は受信を行う。

7．請求の範囲６に記載の通信装置であって、

前記通信手段は、前記他の通信装置から、当該他の通信装置が接続されている第１のルータを一意に識別する第１識別情報を含む前記パケットを受信し、

当該通信装置は、更に、以下を含む：

・ルータ情報取得手段、

当該通信装置が接続されている第２のルータを一意に識別する第２識別情報を取得する；

・判断手段、

前記第１識別情報と前記第２識別情報とが一致するか否か判断する；

・抑制手段、

前記判断手段による判断の結果が否定的である場合に、前記通信手段による前記コンテンツの送受信を抑制する。

8．前記通信手段が送受信する各パケットは、当該通信手段が接続されているネットワークの最大伝送量（Maximum Transmission Unit）に等しいデータサイズであり、且つ、分割して送受信することが禁止されている

ことを特徴とする請求項７に記載の通信装置。

９．前記通信手段は、前記他の通信装置から、送信時に所定ＴＴＬが設定されて送信されたパケットを受信し、

前記取得手段は、前記通信手段が受信した前記パケットからＴＴＬを読み、読み出したＴＴＬと前記所定ＴＴＬとの差分である前記通信距離を取得する

ことを特徴とする請求の範囲８に記載の通信装置。

１０．前記通信手段は、前記他の通信装置から、送信時に前記所定ＴＴＬとして「１」が設定されて送信された前記パケットを受信する

ことを特徴とする請求の範囲９に記載の通信装置。

１１．　前記通信手段は、一部又は全部が暗号化されたパケットを送信又は受信し、

前記暗号処理部は、前記通信手段が受信した前記パケットを復号して前記取得手段へ出力し、又は、前記通信手段により送信されるパケットを暗号化して前記通信手段へ出力する

ことを特徴とする請求の範囲１０に記載の通信装置。

１２．前記取得手段は、当該通信装置と前記他の通信装置との間の長さを示す前記通信距離を取得する

ことを特徴とする請求の範囲１に記載の通信装置。

１３．前記取得手段は、当該通信装置と前記他の通信装置との間のデータ通信に要する時間を示す前記通信距離を取得する

ことを特徴とする請求の範囲１に記載の通信装置。

１４．送信装置から受信装置へ、コンテンツを送信するコンテンツ配信システムであって、

前記送信装置は、以下を含み：

・取得手段、

前記受信装置とのデータ通信における隔たりの量を示す通信距離を取得する；

・判定手段、

取得した前記通信距離が、所定値以下であるか否か判定する；

・送信手段、

前記判定の結果が肯定的である場合に、前記受信手段にコンテンツを送信する；

前記受信装置は、前記送信装置から送信される前記コンテンツを受信する。

１５．通信装置で用いられるコンテンツ配信方法であって、以下を含む：

・取得ステップ、

前記通信装置と他の通信装置とのデータ通信における隔たりの量を示す通信距離を取得する；

・判定ステップ、

取得した前記通信距離が、所定値以下であるか否か判定する；

・通信ステップ、

前記判定の結果が肯定的である場合に、前記他の通信装置との間でコンテンツの送信又は受信を行う。

１６．通信装置で用いられるコンテンツ配信プログラムであって、以下を含む：

・取得ステップ、

前記通信装置と他の通信装置とのデータ通信における隔たりの量を示す通信距離を取得する；

・判定ステップ、

取得した前記通信距離が、所定値以下であるか否か判定する；

・通信ステップ、

前記判定の結果が肯定的である場合に、前記他の通信装置との間でコンテンツの送信又は受信を行う。

１７.通信装置で用いられるコンテンツ配信プログラムを実行するＬＳＩであって、

前記コンテンツ配信プログラムは、以下を含む：

・取得ステップ、

前記通信装置と他の通信装置とのデータ通信における隔たりの量を示す通信距離を取得する；

・判定ステップ、

取得した前記通信距離が、所定値以下であるか否か判定する；

・通信ステップ、

前記判定の結果が肯定的である場合に、前記他の通信装置との間でコンテンツの送信又は受信を行う。

要　約　書

通信途中でコンテンツを盗まれる危険度が高い状況ではコンテンツの送信を抑制するコンテンツ配信システムを提供することを目的とする。

コンテンツサーバは、端末とのデータ通信における隔たりの量を示す通信距離を取得し、前記通信距離が所定値以下である場合に、コンテンツを送受信し前記通信距離が所定値より大きい場合に、コンテンツの送受信を抑制する。